Ruefle, Robin

Robin Ruefle is a member of the technical staff of the CERT Program at the Software Engineering Institute at Carnegie Mellon University. She works as a member of the CERT CSIRT Development team (CDT), which is part of the CERT Education and Training area.

Ruefle's focus is on the development of management, procedural, and technical guidelines and practices for the establishment, maturation, operation, and evaluation of Computer Security Incident Response Teams (CSIRTs) worldwide. As a member of the CSIRT Development Team, Ruefle develops and delivers sessions in the suite of courses offered to CSIRT managers and incident handling staff, including Creating a CSIRT, Managing CSIRTs, Fundamentals of Incident Handling, and Advanced Incident Handling for Technical Staff. She also participates in the Train-the-Trainer program that licenses these products to existing CSIRTs.

The CSIRT Development Team also provides guidance in the development of implementation strategies, policies, standard operating procedures, response plans, and training programs for new and existing CSIRTs. As part of that work, Ruefle has co-authored the following publications: *Handbook for CSIRTs 2nd Edition*, *Organizational Models for CSIRTs Handbook*, *CSIRT Services*, *State of the Practice of CSIRTs*, *Defining Incident Management Processes for CSIRTs: A Work in Progress*, and numerous other articles and guides. These documents can be found at the CERT CSIRT Development web site[http://www.cert.org/csirts/]. She has also presented at numerous incident response and security conferences, including The Forum for Incident Response and Security Teams (FIRST), The US Government Forum for Incident Response and Security Teams (GFIRST), EDUCAUSE, SECURE IT, and other similar forums.

She is currently working with the rest of the CSIRT Development Team on developing a method for assessing CSIRT and incident management operations. As part of this work she co-authored the beta version of the Federal Computer Network Defense (CND) Metrics. The Federal CND Metrics are being developed to provide federal, state, and local agencies with a method for evaluating the effectiveness of an agency's incident management or CSIRT capability (focusing on the Protect, Detect, Respond, and Sustain functions). As part of this work, Ruefle has participated in the assessment and evaluation of various organizations' incident management capabilities.

Ruefle received a BS in political science and an MPIA (Master of Public and International Affairs) from the University of Pittsburgh. She has also taught courses in information technology, management information systems, and information retrieval and analysis as an adjunct faculty member in the Continuing Education and MBA programs at Chatham College and in the Graduate School of Public and International Affairs (GSPIA) at the University of Pittsburgh.

BSI Articles

Name	Content Areas
Defining Computer Security Incident Response Teams	best-practices/incident
The Role of Computer Security Incident Response Teams in the Software Development Life Cycle	best-practices/incident